I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on July 31, 2009.

TOWNSEND and TOWNSEND and CREW LLP

By: / Sally Zumba /

PATENT
Docket No.: 16222U-014110US
Client Ref. No.: P-00895

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Robert W. Seaton, Jr., et al.

Application No.: 10/816,455

Filed: March 31, 2004

For: METHOD AND SYSTEM FOR SECURE AUTHENTICATION

Customer No.: 66945

Confirmation No.: 8400

Examiner: BAYOU, Yonas A.

Art Unit: 2434

STATEMENT OF REASONS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This statement is submitted in support of the Pre-Appeal Brief Request for Review, which is submitted herewith, along with a Notice of Appeal. The Applicant respectfully requests review of the Final Office Action ("FOA") mailed May 5, 2009, regarding the rejection of all pending claims under 35 U.S.C. § 102(b) as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over, *Hodgson* (U.S. Pub. No. 2002/0123972).

Claims 1-8 [*sic*], 10-19, 21-29, and 31-36 [*sic*] are rejected under 35 U.S.C. 102(b) as being anticipated by, or in the alternative, under 35 U.S.C. 103(a) as obvious over Hodgson et al. (U.S. Patent Pub. No. 2002/0123972)("*Hodgson*"). Applicants respectfully submit that *Hodgson* does not disclose each and every limitation of these claims, nor are the claims obvious in view of the single reference.

Claim 36

Claim 36 recites in part, "*generating encryption data, wherein the encryption data comprises a transaction ID, a base redirection url, and an http redirect type, wherein the encryption data further comprises a hashed message authentication code based on the transaction ID, the base redirection URL, and the http redirect type.*" In the rejection of claim 36 there is no mention of such a limitation. (FOA, pg. 9-10). Applicants have reviewed *Hodgson*, and it cannot be determined where "*a hashed message authentication code based on the transaction ID, the base redirection URL, and the http redirect type,*" is disclosed. Furthermore, the FOA has provided no reasoning as to why such a limitation would be obvious in view of *Hodgson*. As such, the FOA has failed to set forth a *prima facie* case for either anticipation or obviousness with respect to claim 36.

Claim 38

Claim 38 recites in part, "*wherein the ACS is further configured to return an authentication response to the merchant server.*" In the rejection of claim 38 there is no mention of such a limitation. (FOA, pg. 9-10). Furthermore, the FOA has provided no reasoning as to why such a limitation would be obvious in view of *Hodgson*. As such, the FOA has failed to set forth a *prima facie* case for either anticipation or obviousness with respect to claim 38.

Claim 18

Claim 18 recites in part, "*the request for the PIN including an instruction to provide the PIN to a destination address.*" The FOA cites *Hodgson* P[0062] and P[0087] as disclosing such a limitation. *Hodgson* P[0087] recites:

> The ***STMS*** 30 automatically sends a follow-up email to the email addressed used to register the PIN/PAD 16. The email contains the transaction information as a confirmation for the consumer.

Aside from containing both the words "*address*" and "*PIN*" *Hodgson* P[0087] does not disclose "*the request for the PIN including an instruction to provide the PIN to a*

destination address." The addition of P[0062] of *Hodgson* does not resolve this discrepancy. *Hodgson* P[0062] recites:

> [**0062**] The STMS **30** determines the correct POS processor **40** to which the transaction request should be sent which is the POS processor used by the bank that provides ATM-Card and Visa/MC services to the merchant. The POS transaction processor **40** has an HSM from the HSM **31**. By providing a means to send the transaction request from the consumer PC **12** to the POS processor **40**, the STMS **30** eliminates the need to send sensitive information such as card information and PIN data to the merchant **20**. Advantageously, the STMS **30** does send the needed credit card/debit card/smart card information to POS transaction processor **40** to request approval for financial transactions.

Hodgson P[0062] does not disclose "*the request for the PIN including an instruction to provide the PIN to a destination address.*" At best, P[0062] generically describes routing of transaction data. The rejection of claim 18 presents no reasoning as to why such a limitation would be obvious in view of *Hodgson.* The FOA does mention such a limitation in the response to arguments section, and in the rejections of claims 1, 6, and 11 (although those claims do not contain such a limitation). The FOA on page 3 (and substantially repeated on page 4) recites:

> relationship with the merchant that the PIN pad user 16 is transacting with. Routing can be driven by an address loaded into the merchant web site and transmitted with each transaction and/or a database maintained at the STMS **[para. 153 and fig. 1**; even though Hodgson does not explicitly teach wherein the request for the PIN includes an instruction to provide the PIN to a destination-address, However, this would have-been obvious, if not even inherent Hodgson already teaches that the PIN is routed to STMS or POS processors, and it would be obvious that this would go to a particular address (it has to go somewhere!)].

As admitted by the FOA, *Hodgson* does not explicitly teach "*the request for the PIN including an instruction to provide the PIN to a destination address.*" With respect to the FOA's argument that such a limitation would be obvious or inherent, the FOA has not set forth a *prima facie* case as to why it would be obvious or inherent. A limitation is only inherently disclosed if it is necessarily present, not by mere possibilities or probabilities. See MPEP 2112(VI). The FOA alleges that because the PIN must go

somewhere, it is inherent that the request for the PIN include a destination address. However, this is not a necessary condition. For example, as shown in Fig. 1 of *Hodgson*, PinPad (28) is only connected to Consumer PC (12). As such, a request from the Consumer PC (12) to the PinPad (28) would not necessarily include a destination address, because the PinPad (28) is not capable of sending the PIN anywhere other than the Consumer PC (12). An instruction to provide the PIN to a destination address would not be necessary in such a situation. As such, the FOA has failed to set forth a *prima facie* case for either anticipation or obviousness in the rejection of claim 18.

Claim 19

Claim 19 recites in part, "*requesting a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) wherein requesting the PIN includes generating a unique transaction identifier, generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier, generating a query having the unique transaction identifier and hash value as fields in the query, and communicating the query.*" There are only two places in *Hodgson* where a PIN is requested. The first is the merchant framework sending a HTML page to the user to instruct the user to enter his PIN. (*Hodgson* P[0070-0072]). The second is where the consumer computer receives the HTML page and processes the page to instruct the user to enter his PIN into the PinPad. (*Hodgson* P[0069-0075]).

With respect to the first request for a PIN, *Hodgson* does not disclose or suggest a hardware security module at the merchant site. As such, it is not possible for the request for a PIN generated at the merchant site to include "*generating a hash value with a front end Hardware Security Module (HSM).*" With respect to the second request for a PIN, *Hodgson* does not disclose the PinPad "*generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier.*" Although *Hodgson* may disclose the PinPad encrypting the credit card number / PIN, encryption and hashing are not the same thing. Encryption ensures privacy, while a hash ensures authenticity. Even if encryption and hashing are considered the same thing,

Hodgson does not disclose or suggest the credit card number / PIN is encrypted "*based in part on the unique transaction identifier.*"

The Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a *prima facie* case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 19 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 19, and the claims which depend therefrom, is respectfully requested.

Claim 1

As encouraged by the instructions for preparation of the pre-appeal conference brief, applicants refer to arguments of record with respect to claim 1. More specifically, please refer to the arguments presented in the Response to Office Action filed February 13, 2009, at pages 10-12.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

Respectfully submitted,

/Preetam B. Pagar/

Preetam B. Pagar
Reg. No. 57,684

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (415) 576-0200 / Fax: (415) 576-0300
PBP:pbp